



Cybersecurity Update

Gary Foster
April 10, 2017



Discussion Topics

- **Cybersecurity Challenges**
- **Policy Work**
- **Security Awareness & Training**
- **Execution of Policies**
- **Next Steps**



4/10/2017

Cybersecurity Challenges



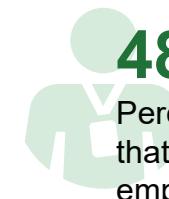
38%↑

Increase in cybersecurity incidents in the past year.¹



5 Months

Average time it takes to detect a security breach.²



48%

Percentage of data breaches that are caused by employees and contractors.²



A complex, moving target

Cyber threats are an increasing risk for MassDOT as professional hackers execute ever more sophisticated attacks against government agencies and private sector companies.



Commonwealth and MassDOT priority

The Commonwealth and MassDOT have identified cybersecurity as top priority. Cybersecurity is critical to MassDOT's ongoing ability to successfully perform its mission.



Cybersecurity begins with us

Cybersecurity is not simply an IT issue, it is an enterprise-wide responsibility. To successfully prevent, identify, and address cybersecurity threats, everyone's involvement is imperative.



4/10/2017

¹ PwC Global State of Information Security Survey

² Ponemon Institute

Policy Work

1 Access Control & Identification and Authentication. User account management, access enforcement and monitoring, separation of duties, and remote access.	How do we ensure employees have the appropriate accesses to the correct information?
2 Awareness and Training. Timing, frequency, assignment, and documentation of security awareness and role-based security trainings.	Are employees aware of their responsibilities to protect confidential information?
3 Audit and Accountability. Audit process controls, including the definition of auditable events, coordination of the audit function and processes, and management of audit records.	Are mechanisms in place to track activities performed on our systems?
4 Security and Risk Assessment. Scope, frequency, and goals of security and risk assessments.	How do we measure the effectiveness of our information system security?
5 Configuration Management and goals of the config information systems.	How can we ensure information is protected when using removable media?
6 Contingency Planning. maintenance of a cont. information systems.	How can we ensure our facilities are protected from physical threats such as fires and thefts?
7 Incident Response. Plan and implementation of response plan.	How can we evolve with an ever-changing information system security landscape?
8 Maintenance. Scope, information system management, timely, secure, and eff.	How do we mitigate risks associated with employee and contractor access to sensitive information systems?
9 Systems and Services Acquisition. Acquisition of systems and services, as well as controls around software development.	How can we ensure information security and proactively mitigate associated risks during systems acquisition/commissioning?
10 System and Communication Protection. Protection of MassDOT's network and resources, and securing of communications across the network.	How can we safely transmit and process sensitive information during day-to-day business operations?
11 System and Information Integrity. Maintain system integrity, identifying system flaws, and protecting the system from malicious activity.	What controls should be in place to protect MassDOT and MBTA information systems from malicious code?
12 Data Classification. Classification of critical data elements and defines controls for these sensitive data types.	How should we assign our limited budget to ensure the highest possible level of protection?

16

Information security policies created...

189

Internal controls developed...

100%

Policies and internal controls have been signed off as draft by MassDOT senior leadership for implementation

The first policy to be implemented is Security Awareness & Training.



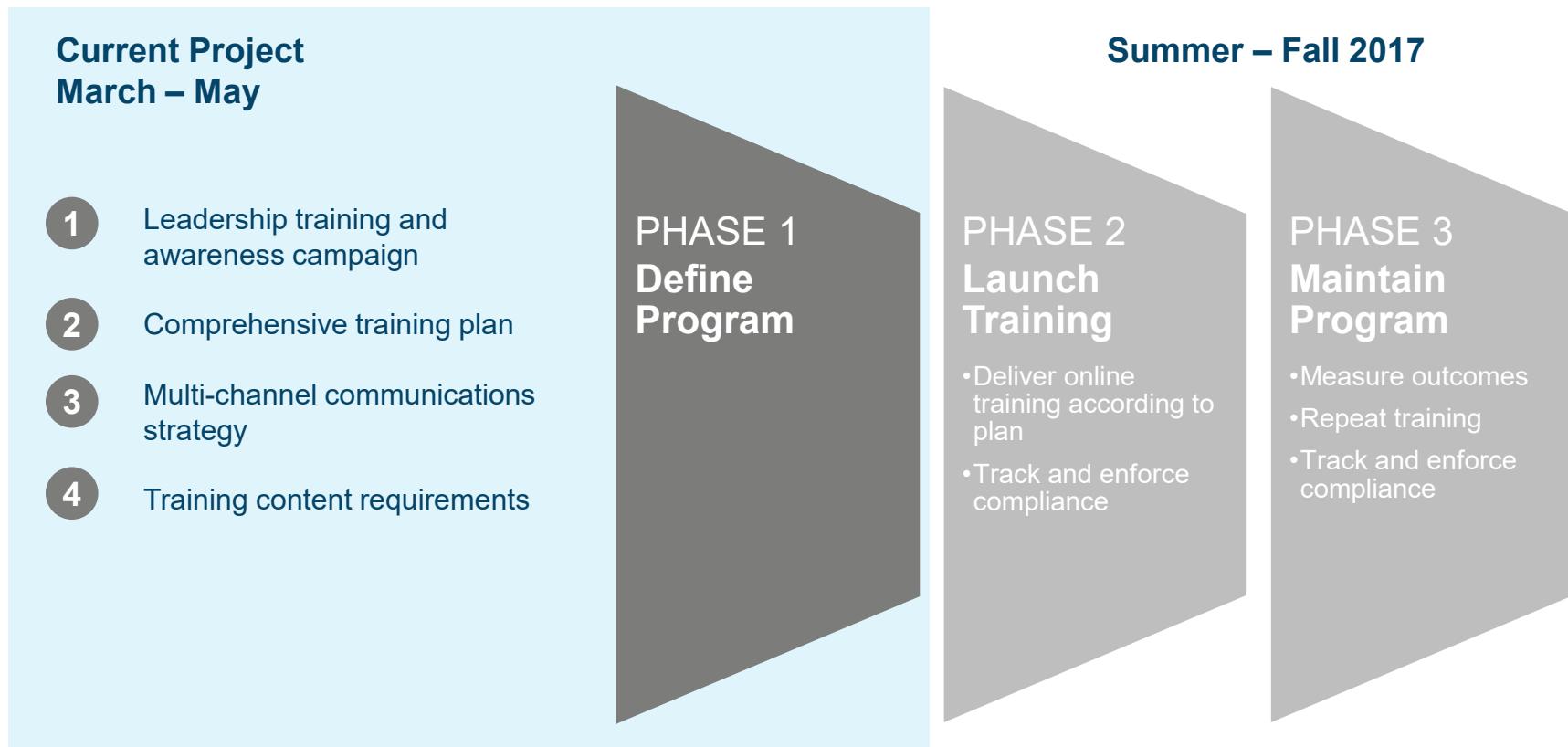
4/10/2017

4



Security Awareness & Training

The Security Awareness & Training program is being delivered in three phases. Phase 1, the current project, defines the program and establishes the approach for subsequent work.



4/10/2017

5



Execution of Policies

Based on a survey distributed to MassDOT information system users, respondents see cybersecurity as important, and are receptive to training and additional knowledge.



Of the comments provided, 41% related to the need to change current practices; *passwords* were the most frequently cited pain point.

41%



39%



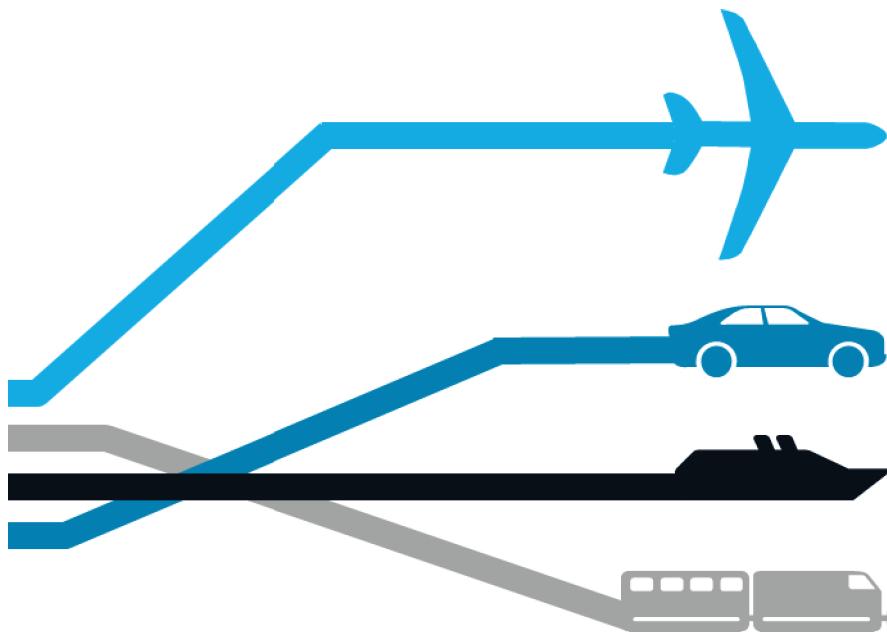
*Surface area of graphics are scaled to match percentage proportions

4/10/2017



Next Steps

There are several components that are essential to the success of the Security Awareness & Training program.



Leadership support

Will be essential for communicating the value of the program and gaining buy-in

Receptive adoption

Change management is crucial to successfully implementing the training and adopting cybersecurity best practices

Enterprise-wide involvement

Cybersecurity needs to be the responsibility of every division, not only IT

Ongoing input

With your continued input, the implementation will have best chance at succeeding short-term and being sustainable long-term



4/10/2017

7

